PORTARIA Nº 201/2021/SEI-CEMADEN, DE 16 DE SETEMBRO DE 2021

Institui a Política de Segurança da Informação (POSIN) no âmbito do Centro Nacional de Monitoramento e Alertas de Desastres Naturais (CEMADEN).

O DIRETOR do Centro Nacional de Monitoramento e Alertas de Desastres Naturais – CEMADEN, nomeado por meio da Portaria nº 998, de 3 de junho de 2015, publicada na Seção 2, do DOU nº 105, dia 5 de junho de 2015, apostilada pela Portaria nº 5197 /2016/SEI-MCTIC, de 14 de novembro de 2016, publicada no Boletim de Serviço nº 21-A, de 14 de novembro de 2016, reconduzido por meio da Portaria nº 15, de 2 de janeiro de 2020, publicada na Seção 2, do DOU nº 03, dia 6 de janeiro de 2020, no uso da competência atribuída no artigo 26, Anexo, da Portaria nº 3.441, de 10 de setembro de 2020, publicada no DOU nº 175-B, Seção I - Extra, de 11 de setembro de 2020, **RESOLVE:**

Art. 1º - APROVAR a Política de Segurança da Informação (POSIN) do Centro Nacional de Monitoramento e Alertas de Desastres Naturais (CEMADEN), nos termos do Anexo desta Portaria.

Art. 2º - ESTABELECER o prazo de 30 (trinta) dias para que os Titulares das unidades organizacionais do Cemaden submetam para apreciação da Direção o nome de 01 (um) representante de sua área para composição do Comitê de Segurança da Informação e Comunicações de Dados (CSIC) do CEMADEN.

Art. 3º - Esta Portaria entra em vigor na data de sua publicação.

OSVALDO LUIZ LEAL DE MORAES
Diretor

ANEXO DA PORTARIA Nº 201/2021

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO CENTRO NACIONAL DE MONITORAMENTO E ALERTAS DE DESASTRES NATURAIS

1. OBJETIVO

1.1. A Política de Segurança da Informação (POSIN) tem por objetivo a instituição de diretrizes estratégicas que visam garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações, bem como atitudes adequadas para manuseio, tratamento, controle e proteção dos dados, informações, documentos e conhecimentos produzidos, armazenados, sob guarda ou transmitidos por qualquer meio ou recurso do Centro Nacional de Monitoramento e Alertas de Desastres Naturais (CEMADEN), contra ameaças e vulnerabilidades. Desse modo, esta política busca preservar os seus ativos de informação, assim como a sua imagem institucional.

1.2. O propósito desta política é estabelecer diretrizes estratégicas para orientar e apoiar as ações institucionais em segurança do CEMADEN no que diz respeito à gestão de riscos e ao tratamento de incidentes de Segurança da Informação e Comunicações de Dados

(SIC), em conformidade com as disposições constitucionais, legais e regimentais vigentes.

1.3. A POSIN estabelece o comprometimento da alta direção organizacional da empresa, com vistas a prover apoio para a implantação da Gestão de Riscos da Segurança da Informação e Comunicações de Dados (GRSIC).

2. ESCOPO

2.1. Esta POSIN aplica-se ao CEMADEN, sendo de responsabilidade de todos os servidores, estagiários, bolsistas e colaboradores internos ou externos, permanentes, temporários ou eventuais, devendo ser dado amplo conhecimento de seu teor a todas as pessoas ou organizações que utilizam os meios físicos ou lógicos do CEMADEN, por serem todos responsáveis por garantir a segurança das informações a que tenham acesso.

3. CONCEITOS E DEFINIÇÕES

3.1. Para efeitos desta POSIN são estabelecidos os significados dos seguintes termos e expressões:

I. Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade. (Ref.: NC07/IN01/DSIC/GSIPR/2010)

II. Acesso lógico: acesso a redes de computadores, serviços e sistemas computacionais, de comunicação de dados e estações de trabalho, fixas ou móveis, com ou sem a necessidade de autenticação.

III. Acesso remoto: funcionalidade que permite acesso ao conteúdo ou controle de um determinado computador através da Internet.

IV. Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização. (Ref.: 04/IN01/DSIC/GSI/PR/2013)

V. Ativo de informação: qualquer componente (humano, tecnológico, físico ou lógico) que sustenta um ou mais processos de negócio de uma unidade ou área de negócio. Inclui meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

VI. Auditoria: atividade que engloba o exame das operações, processos, sistemas e responsabilidades gerenciais, com o intuito de verificar sua conformidade com os objetivos e políticas institucionais, orçamentos, regras, normas e padrões.

VII. Autenticidade: qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema. (Ref.: Lei nº 12.527/2011)

VIII. Colaborador: pessoa jurídica ou pessoa física que desempenhe serviço, em caráter permanente, temporário ou eventual.

IX. CSIC: Comitê de Segurança da Informação e Comunicações de Dados, instituído no âmbito do CEMADEN, com a responsabilidade de assessorar a implementação das ações de SIC.

X. Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado.

XI. Continuidade de negócio: capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e

recuperando perdas de ativos de informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido.

XII. Custodiante do ativo de informação: aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia.

XIII. Desastres: evento repentino e não planejado que causa perda para toda ou parte da organização e gera sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação. (Ref.: NC06/IN01/DSIC/GSIPR/2009)

XIV. Disponibilidade: qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados. (Ref.: Lei nº 12.527/2011)

XV. ETIR: Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais, grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores. (Ref.: NC03/IN01/DSIC/GSIPR/2009)

XVI. Incidente de segurança: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores. (Ref.: 05/IN01/DSIC/GSIPR/2009)

XVII. Integridade: qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino. (Ref.: Lei nº 12.527/ 2011)

XVIII. GRSIC: Gestão de riscos de Segurança da Informação e Comunicações de Dados, é um conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos.

XIX. Licença Demo: licença de um aplicativo reproduzido parcialmente para que o usuário possa avaliar o programa antes da aquisição.

XX. Licença Shareware: licença em que um aplicativo também é colocado em circulação para avaliação permitindo que o programa possa ser usado durante um período de tempo determinado para logo após ser retirado do computador.

XXI. Licença Trial: o mesmo que Licença Demo.

XXII. Política de Segurança - conjunto de diretrizes destinadas a definir a proteção adequada dos ativos produzidos pelos Sistemas de Informação das entidades.

XXIII. Política de Segurança da Informação - documento aprovado pela autoridade responsável pelo órgão ou entidade da APF, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da SI (Este termo substituiu o termo Política de Segurança da Informação e Comunicações).

XXIV. POSIC - acrônimo de Política de Segurança da Informação e Comunicações. Foi substituído pelo acrônimo POSIN.

XXV. POSIN - acrônimo de Política de Segurança da Informação. Substituiu o acrônimo POSIC.

XXVI. Princípios: são ideias centrais que estabelecem diretrizes a um dado sistema, conferindo-lhe um sentido lógico, harmonioso e racional.

XXVII. Quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações de dados.

XXVIII. Risco: risco, na área de SIC, é o potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização.

XXIX. Sensibilização em SIC: saber o que é segurança da informação e comunicações de dados aplicando em sua rotina pessoal e profissional.

XXX. SIC: Segurança da Informação e Comunicações de Dados, ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações. (Ref.: IN GSI/PR 01/2008)

XXXI. SPAM: termo usado para referir-se aos *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas.

XXXII. Terceiros: quaisquer pessoas, físicas ou jurídicas, de natureza pública ou privada, externos ao CEMADEN.

XXXIII. Tratamento da informação: conjunto de ações referentes à produção, classificação, utilização, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação. (Ref.: Lei nº 12.527/ 2011)

XXXIV. Usuário: agente público, auditores e quaisquer outros entes que podem acessar ativos de informação do CEMADEN mediante autorização de gestores de ativos;

XXXV. Vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação. (Ref.: NC04/IN01/DSIC/GSIPR/2013)

4. REFERÊNCIAS LEGAIS E NORMATIVAS

4.1. Esta Política de Segurança da Informação do Centro Nacional de Monitoramento e Alertas de Desastres Naturais (POSIN/CEMADEN) observa a legislação e as normas específicas, destacando-se:

I. Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a Política Nacional de Arquivos Públicos e privados e dá outras providências;

II. Lei nº 8.745, de 9 de dezembro de 1993, que dispõe sobre a contratação por tempo determinado para atender a necessidade temporária de excepcional interesse público, nos termos do inciso IX do art. 37 da Constituição Federal, e dá outras providências;

III. Lei nº 9.962, de 22 de fevereiro de 2000, que disciplina o regime de emprego público do pessoal da Administração federal direta, autárquica e fundacional, e dá outras providências;

IV. Lei nº 9.983, de 14 de julho de 2000, que altera o Decreto-Lei nº 2.848, de 7 de setembro de 1940 (Código Penal), que dispõe sobre a tipificação de crimes por computador contra a Previdência Social e a Administração Pública;

V. Art. 1.016 da Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil), que dispõe que os administradores respondem solidariamente perante a sociedade e os terceiros prejudicados, por culpa no desempenho de suas funções;

VI. Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto no inciso XXXIII do art. 5º no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de

maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências;

VII. Lei nº 13.709, de 14 de agosto de 2018, que estabelece a Lei Geral de Proteção de Dados Pessoais (LGPD);

VIII. Decreto nº 1.171, de 22 de junho de 1994, que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;

IX. Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

X. Decreto nº 4.073, de 3 de janeiro de 2002, que regulamenta a Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a Política Nacional de Arquivos Públicos e Privados;

XI. Decreto nº 7.724, de 16 de maio de 2012, que regulamenta a Lei nº 12.527, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição;

XII. Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

XIII. Decreto nº 9.756, de 11 de abril de 2019, que institui o portal único “gov.br” e dispõe sobre as regras de unificação dos canais digitais do Governo federal;

XIV. Portaria nº 4.711, de 18 de agosto de 2017, do Ministério da Ciência, Tecnologia, Inovações e Comunicações, que aprova a Política de Segurança da Informação e Comunicações do Ministério da Ciência, Tecnologia, Inovações e Comunicações (Posic/MCTIC) e revoga a Portaria MCTI nº 208, de 11 de março de 2016, e a Portaria MC nº 1410, de 18 de setembro de 2014;

XV. Resolução nº 20, de 16 de julho de 2004, do Conselho Nacional de Arquivos, que dispõe sobre a inserção dos documentos digitais em programas de gestão arquivística de documentos dos órgãos e entidades integrantes do Sistema Nacional de Arquivos;

XVI. Resolução nº 32, de 17 de maio de 2010, do Conselho Nacional de Arquivos, que dispõe sobre a inserção dos metadados na Parte II do modelo de requisitos para sistemas informatizados de gestão arquivística de documentos - eARQ Brasil;

XVII. Câmara Técnica de Documentos Eletrônicos. Conselho Nacional de Arquivos. e-ARQ Brasil: modelo de requisito para sistemas informatizados de gestão arquivística de documentos. Rio de Janeiro: Arquivo Nacional, 2011. v. 1.1;

XVIII. Câmara Técnica de Documentos Eletrônicos. Conselho Nacional de Arquivos. Glossário de termos técnicos (v5). 2010b;

XIX. Instrução Normativa nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

XX. Instrução Normativa nº 02, de 5 de fevereiro de 2013, do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre o credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal;

XXI. Instrução Normativa nº 03, de 6 de março de 2013, do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre os parâmetros e padrões mínimos dos

recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal;

XXII. Norma Complementar nº 04 da IN 01, de 15 de fevereiro de 2013, do Gabinete de Segurança Institucional da Presidência da República, que estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) nos órgãos ou entidades da Administração Pública Federal (APF), direta e indireta;

XXIII. Norma Complementar nº 05 da IN 01, de 14 de agosto de 2009, do Gabinete de Segurança Institucional da Presidência da República, que disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais (ETIR) nos órgãos e entidades da Administração Pública Federal;

XXIV. Norma Complementar nº 06 da IN 01, de 11 de novembro de 2009, do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre a gestão de continuidade de negócios em segurança da informação e comunicações;

XXV. Norma Complementar nº 07 da IN 01, de 15 de julho de 2014, do Gabinete de Segurança Institucional da Presidência da República, que estabelece diretrizes para implementação de controles de acesso relativos à segurança da informação e comunicações;

XXVI. Norma Complementar nº 09 da IN 01, de 15 de fevereiro de 2013, do Gabinete de Segurança Institucional da Presidência da República, que estabelece orientações específicas para o uso de recursos criptográficos em segurança da informação e comunicações;

XXVII. Norma Complementar nº 10 da IN 01, de 30 de janeiro de 2012, do Gabinete de Segurança Institucional da Presidência da República, que estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta - APF;

XXVIII. Norma Complementar nº 11 da IN 01, de 30 de janeiro de 2012, do Gabinete de Segurança Institucional da Presidência da República, que estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta - APF;

XXIX. Norma Complementar nº 12 da IN 01, de 30 de janeiro de 2012, do Gabinete de Segurança Institucional da Presidência da República, que estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta;

XXX. Norma Complementar nº 13 da IN 01, de 30 de janeiro de 2012, do Gabinete de Segurança Institucional da Presidência da República, que estabelecer diretrizes para a Gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta (APF);

XXXI. Norma Complementar nº 14 da IN 01, de 13 de março de 2018, do Gabinete de Segurança Institucional da Presidência da República, que estabelece princípios, diretrizes e responsabilidades relacionados à Segurança da Informação (SI) para o tratamento de informação em ambiente de Computação em Nuvem, nos órgãos e entidades da Administração Pública Federal, direta e indireta (APF);

XXXII. Norma Complementar nº 15 da IN 01, de 11 de junho de 2012, do Gabinete de Segurança Institucional da Presidência da República, que estabelecer diretrizes de Segurança da Informação e Comunicações para o uso das redes sociais, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta;

XXXIII. Norma Complementar nº 16 da IN 01, de 21 de novembro de 2012, do Gabinete de Segurança Institucional da Presidência da República, que estabelecer diretrizes de Segurança da Informação e Comunicações para a obtenção de software seguro nos órgãos e entidades da Administração Pública Federal, direta e indireta;

XXXIV. Norma Complementar nº 17 da IN 01, de 09 de abril de 2013, do Gabinete de Segurança Institucional da Presidência da República, que estabelece diretrizes nos contextos de atuação e adequações para profissionais da área de Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta (APF);

XXXV. Norma Complementar nº 18 da IN 01, de 09 de abril de 2013, do Gabinete de Segurança Institucional da Presidência da República, que estabelece diretrizes para as atividades de ensino em Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;

XXXVI. Norma Complementar nº 19 da IN 01, de 15 de julho de 2014, do Gabinete de Segurança Institucional da Presidência da República, que estabelece padrões mínimos para a segurança da informação e comunicações dos sistemas estruturantes nos órgãos e entidades da Administração Pública Federal, direta e indireta;

XXXVII. Norma Complementar nº 20 da IN 01, de 15 de dezembro de 2014, do Gabinete de Segurança Institucional da Presidência da República, que estabelece diretrizes de Segurança da Informação e Comunicações (SIC) para instituição do processo de tratamento da informação, envolvendo todas as etapas do ciclo de vida da informação, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta;

XXXVIII. Norma Complementar nº 21 da IN 01, de 08 de outubro de 2014, do Gabinete de Segurança Institucional da Presidência da República, que estabelecer diretrizes para o registro, coleta e preservação de evidências de incidentes de segurança em redes computacionais dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF e a comunicação às autoridades competentes.

XXXIX. NBR ISO/IEC 27001:2006: Sistemas de gestão de segurança da informação;

XL. NBR ISO/IEC 27002:2007: Código de prática para a gestão da segurança da informação.

5. PRINCÍPIOS

5.1. São princípios básicos desta POSIN:

a) A preservação da imagem do Órgão e de seus colaboradores.

b) A proteção dos dados pessoais de seus colaboradores.

c) A garantia ao direito pessoal e coletivo à intimidade e ao sigilo da correspondência, das comunicações e transferências de dados individuais.

d) A proteção dos dados, informações e conhecimentos produzidos no CEMADEN classificados como sigilosos.

e) A disseminação da cultura de Segurança da Informação e Comunicações de Dados (SIC).

f) Que o nível, a complexidade e os custos das ações de Segurança da Informação e Comunicações de Dados (SIC) sejam adequados ao valor dos ativos e informações, considerando os riscos a que estão expostos.

g) Que as ações de Segurança da Informação e Comunicações de Dados do CEMADEN sejam integradas com os objetivos de negócio, com as demais ações dos órgãos da administração pública e sociedade civil e estejam alinhas às diretrizes nacionais de segurança da informação.

6. DIRETRIZES GERAIS

6.1. A segurança da informação e comunicações de dados tem como principal diretriz a proteção da informação, garantindo a continuidade do negócio, minimizando seus riscos, maximizando o retorno sobre os investimentos e as oportunidades pertinentes. (Ref. ISO/IEC 27.002:2006)

6.2. As diretrizes de segurança da informação e comunicações de dados descritas nesta POSIN devem ser observadas por todos os colaboradores que executem atividades vinculadas a esta instituição durante todas as etapas do tratamento da informação, a saber: produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.

6.3. As diretrizes de segurança da informação e comunicações de dados devem considerar, prioritariamente, objetivos estratégicos, processos, requisitos legais e a estrutura do CEMADEN.

6.4. Os recursos tecnológicos, as instalações de infraestrutura, sistemas de informação e as aplicações devem ser protegidos contra indisponibilidade, acessos indevidos, falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas.

6.5. É condição para acesso aos ativos de informação do, ou custodiados pelo, CEMADEN a adesão formal aos termos desta POSIN, mediante assinatura de Termo de Responsabilidade.

6.6. O princípio da economicidade na proteção dos ativos de informação deve ser observado.

6.7. Devem ser observados a pessoalidade e utilidade do acesso aos ativos de informação.

6.8. É vedado comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pelo CEMADEN.

6.9. Cópias de documentos classificados deverão sofrer o mesmo processo de classificação de seu original.

6.10. O custodiante do ativo de informação deve ser formalmente designado pelo proprietário do ativo de informação. A não designação pressupõe que o proprietário do ativo de informação é o próprio custodiante.

6.11. O custodiante será responsabilizado pelos atos que comprometam a segurança do sistema da informação advindos de suas credenciais ou ativos sob sua custódia.

6.12. Os contratos, convênios, acordos e instrumentos congêneres firmados pelo CEMADEN devem conter cláusulas que determinem a observância desta Política e seus documentos complementares.

7. DIRETRIZES ESPECÍFICAS

7.1. Para cada uma das diretrizes deste capítulo deve ser observada a pertinência de elaboração de políticas, procedimentos, normas, orientações e/ou manuais que disciplinem ou facilitem o seu entendimento.

7.2. Tratamento da Informação

7.2.1. As informações geradas, adquiridas ou custodiadas sob a responsabilidade do CEMADEN são consideradas parte do seu patrimônio intelectual não cabendo a seus criadores qualquer forma de direito autoral, salvo aqueles direitos garantidos no âmbito da Lei de Inovação e outros dispositivos legais, e devem ser protegidas segundo as diretrizes descritas nesta Política, em seus documentos complementares e demais regulamentações em vigor.

7.2.2. Informações geradas, adquiridas ou custodiadas pelo CEMADEN podem possuir classificação para indicar a necessidade, a prioridade e o nível esperado de proteção quanto ao seu tratamento.

7.2.3. Quando classificadas, serão observadas as exigências das atividades da instituição, considerando as implicações que um determinado grau de classificação trará para os seus objetivos institucionais, observando a legislação em vigor.

7.2.4. Nos termos da Lei de Acesso à Informação (Lei n° 12.527, de 18 de novembro de 2011), é vedada a divulgação e uso por terceiros de informações restritas ou classificadas por grau de sigilo, produzidas ou custodiadas pelo CEMADEN, salvo nos casos de autorização específica.

7.2.5. O cumprimento dessa Política, bem como das normas complementares e procedimentos de SIC no CEMADEN será auditado periodicamente, de acordo com os critérios definidos pelo Comitê de Segurança da Informação e Comunicações de Dados (CSIC), vinculado diretamente à Diretoria do CEMADEN.

7.2.6. O acesso às informações, sistemas e instalações depende da apresentação de identificador único, pessoal, intransferível e com validade estabelecida, que permita de maneira clara e indiscutível o seu reconhecimento.

7.2.7. A área de Tecnologia da Informação e Comunicações de Dados deve estabelecer critérios de segurança para o desenvolvimento, manutenção e aquisição de sistemas e aplicações.

7.2.8. Para garantir o cumprimento das normas, os responsáveis pelas unidades deverão auxiliar no controle do uso dos recursos computacionais.

7.3. Segurança em Recursos Humanos

7.3.1. As responsabilidades pela segurança da informação devem ser definidas pelo CSIC.

7.3.2. Todos os usuários devem ser conscientizados e treinados nos procedimentos de SIC.

7.3.3. O controle operacional de uma atividade crítica não pode ser atribuição exclusiva de uma única pessoa devendo, sempre que possível, ser atribuída à unidades organizacionais, setores ou grupos.

7.3.4. Quando do afastamento, mudança de responsabilidades e de lotação ou atribuições dentro da organização, faz-se necessária a revisão imediata dos direitos de acesso e uso dos ativos.

7.3.5. Quando da efetivação do desligamento de usuário, deverão ser extintos todos os direitos de acesso e uso dos ativos a ele atribuído.

7.3.5.1. A critério do Titular da unidade responsável pelo usuário desligado, poderá ser estipulado um período de até 15 (quinze) dias de extensão na validade das contas para efetivação de eventual transferência de conhecimento.

7.3.5.2. Usuários categorizados como Bolsistas terão, automaticamente, um período de 15 (quinze) dias de extensão na validade de suas contas, tendo por objetivo evitar a descontinuidade dos acessos durante o período de eventual renovação do vínculo.

7.3.6. Todo ativo produzido pelo usuário, desligado, deverá ser mantido pelo CEMADEN garantindo o reconhecimento e o esclarecimento da propriedade do acervo para Instituição.

7.3.7. O usuário desligado tem por direito exigir as garantias estabelecidas na Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais.

7.4. **Gestão de Ativos de TIC**

7.4.1. Os ativos de TIC são propriedade do CEMADEN e devem ser catalogados e registrados e, caso seja um objeto físico, deve ser patrimoniado pelo CEMADEN e geridos conforme disposto no Regimento Interno do Órgão.

7.4.2. Os ativos de TIC possuem um responsável e podem ser custodiados a terceiros mediante autorização do Titular da unidade competente e expresso consentimento do custodiante.

7.4.3. A responsabilidade sobre os ativos é solidária entre o Responsável pelo ativo e o Custodiante do ativo.

7.4.4. O custodiante e o responsável por determinado ativo devem zelar pelo ativo e garantir sua correta utilização e preservação.

7.4.5. O CSIC deverá deliberar sobre o uso desses ativos fora do ambiente Institucional.

7.5. **Tratamento de Incidentes de Rede**

7.5.1. O Presidente do Comitê de Segurança da Informação e Comunicações de Dados deverá instituir a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), em conformidade com a Instrução Normativa GSI/PR nº 1 e a Norma Complementar nº 05/IN01/DSIC/GSIPR.

7.5.2. A gestão de incidentes de segurança da informação será regulamentada por norma específica.

7.6. **Gestão de Risco**

7.6.1. As unidades responsáveis por ativos de informação devem implantar processos contínuos de gestão de riscos, os quais serão aplicados na implementação e operação da gestão da segurança da informação e comunicações de dados.

7.6.2. A Gestão de Riscos da Segurança da Informação e Comunicações de Dados (GRSIC) deve avaliar os riscos relativos à segurança dos ativos de informação e a conformidade com exigências regulatórias ou legais.

7.6.3. A GRSIC será regulamentada por norma específica.

7.7. **Gestão de Continuidade**

7.7.1. O Comitê de Segurança da Informação e Comunicações de Dados (CSIC) poderá instituir, formalmente, grupo de trabalho com objetivo de propor, manter e periodicamente testar medidas de gestão da continuidade e recuperação da informação, visando reduzir para um nível aceitável ou previamente definido a possibilidade de interrupção ou o impacto causado por desastres nos recursos de tecnologia da informação e comunicações que suportam os processos vitais do CEMADEN, até que se retorne à normalidade.

7.7.2. A gestão de continuidade de negócio será regulamentada por norma específica

7.8. **Auditoria e Conformidade**

7.8.1. A verificação de conformidade das práticas de SIC deverá ser realizada sempre que necessária, não excedendo o período máximo de 3 (três) anos.

7.8.2. A verificação da conformidade será realizada de forma planejada, mediante calendário de ações aprovado pelo CSIC.

7.8.3. A verificação de conformidade deve também ser realizada nos contratos, convênios, acordos de cooperação e outros instrumentos do mesmo gênero celebrados com o CEMADEN.

7.8.4. A execução da verificação de conformidade será realizada por grupo de trabalho formalmente instituído pelo CSIC, podendo, com a prévia aprovação deste, ser subcontratada no todo ou em parte.

7.8.5. É vedado ao prestador de serviços executar a verificação da conformidade dos próprios serviços prestados.

7.8.6. Os resultados de cada ação de verificação de conformidade serão documentados em relatório de avaliação de conformidade e, com base neste, o Presidente do Comitê de Segurança da Informação e Comunicações de Dados tomará medidas cabíveis.

7.9. **Controles de Acesso Físico e Lógico**

7.9.1. O acesso físico às dependências do CEMADEN é público e livre, exceto aos setores classificados como sendo de operação crítica.

7.9.2. As áreas correspondentes às salas de Telecomunicações, Datacenter (Centro de Processamento de Dados e Sala de Servidores), Elétrica e Sala de Situação são considerados como setores de operações críticas e devem possuir acesso controlado.

7.9.3. O acesso lógico aos recursos do CEMADEN (incluindo equipamentos de Informática e telecomunicações) deverá contemplar os diversos perfis e necessidades dos usuários e projetos desenvolvidos no Centro.

7.9.4. Os perfis de acesso devem ser elaborados e definidos pelo CSIC.

7.9.5. As coordenações são responsáveis pelos colaboradores a ela vinculadas de forma direta ou indireta e devem informar ao CSIC quaisquer mudanças no perfil de seus colaboradores.

7.9.6. O CSIC deverá estabelecer os procedimentos e metodologias necessários para aplicação do controle de acesso físico e lógico, bem como definir e reavaliar as definições de criticidade das demais áreas e sistemas.

7.10. **Uso de softwares**

7.10.1. Todos os softwares a serem instalados no CEMADEN devem dispor de autorização para uso comercial, empresarial ou governamental ou possuir licença de uso gratuita tendo sido adquiridos para uso nas atividades e projetos do CEMADEN.

7.10.2. A instalação de licenças de software adquiridas para outras instituições ou individualmente deverão ser avaliadas e autorizadas pelo CSIC.

7.10.3. Os softwares com licença do tipo TRIAL, DEMO, SHAREWARE ou similares, que dispõem de um período de avaliação, podem ser instalados desde que respeitados os termos de suas licenças. Após expirados os prazos de utilização desses softwares, para que seu uso possa continuar, se faz necessário a aquisição da licença do software.

7.10.4. O CSIC, com o apoio, se necessário, das equipes técnicas do CEMADEN, deverá estabelecer critérios para avaliar a implementação e uso dos softwares.

7.10.5. O CSIC poderá, à qualquer momento, restringir o uso de algum software no âmbito do CEMADEN, caso seja considerado um risco à segurança da Informação do Órgão ou de seus colaboradores e parceiros.

7.10.6. É vedada a instalação, configuração ou uso de softwares que não possuam licença ou permissão para uso comercial ou empresarial, podendo tais atos serem enquadrados na Lei Nº 10.695, de 2 de julho de 2003, que altera o Código Penal e dispõe sobre os crimes de violação de direito de autor e dos direitos conexos.

7.10.7. Os usuários, com a devida anuência do Titular da unidade em que estiverem vinculados, poderão solicitar que seus perfis de acesso tenham permissões para instalação de softwares nos computadores que estiverem utilizando.

7.10.7.1. Esta autorização será concedida mediante assinatura de Termo de Responsabilidade, que também conterá a assinatura do Titular de sua unidade.

7.10.7.2. Não estão contemplados nesta autorização os computadores de uso inerentemente compartilhado e de missão crítica do CEMADEN, como os das Salas de Situação.

7.10.7.3. O CSIC poderá, à qualquer momento, suspender as autorizações dos usuários que violarem as normas de segurança vigentes, em especial as estabelecias nesta POSIN, e encaminhar os fatos que levaram à suspensão para a apuração das autoridades competentes.

7.11. **Uso de correio eletrônico**

7.11.1. O serviço de correio tem como finalidade o envio e o recebimento eletrônico de mensagens e documentos relacionados com as funções e atividades institucionais do CEMADEN.

7.11.2. O correio eletrônico é oferecido como um serviço do CEMADEN, sendo a custódia de cada conta oferecida a um determinado colaborador. Sendo assim, cabe à cada custodiante a administração e manutenção de suas contas.

7.11.3. É vedado o uso do email institucional para fins de cadastro ou criação de contas em sistemas e formulários que estejam em desacordo com as finalidades, projetos, ações, atividades ou parcerias do CEMADEN.

7.11.4. É vedado o acesso de terceiros ao conteúdo das mensagens tramitadas por meio do serviço de correio eletrônico institucional, salvo nas hipóteses previstas em lei.

7.11.5. É vedado o uso de e-mail institucional para o disparo massivo de mensagens que possa vir a ser caracterizado como envio de mensagem não-solicitada ou indesejada (SPAM).

7.11.6. O CSIC deverá estabelecer as normas específicas e os procedimentos de uso de correio eletrônico, bem como as sanções para os casos de infrações, observando a legislação em vigor.

7.12. **Acesso a Internet, Intranet e Redes Sociais**

7.12.1. O acesso à Internet é de caráter prioritariamente profissional, com conteúdo relacionado às atividades desempenhadas pelo Órgão, observando-se sempre a conduta compatível com a moralidade administrativa.

7.12.2. Cada usuário é responsável pelas ações e acessos realizados por meio da sua Conta de Acesso.

7.12.3. O acesso à páginas da Internet é livre, nos termos desta POSIN, no âmbito do CEMADEN, salvo restrições aplicadas pelo CSIC observando a necessidade das atividades e sua pertinência.

7.12.4. Cabe ao CSIC estabelecer os níveis de acesso e restrições para cada perfil.

7.12.4.1. A atribuição dos perfis para os colaboradores será feita, ou alterada, a qualquer momento, por solicitação dos Titulares de cada unidade.

7.13. **Portal e Redes Sociais Institucionais**

7.13.1. O Portal Institucional deve seguir a Identidade Digital de Governo estabelecido pelo portal padrão (http://www.portalpadrao.gov.br/).

7.13.2. É permitido ao CEMADEN possuir perfil institucional em redes sociais.

7.13.3. Perfis institucionais mantidos nas redes sociais devem, preferencialmente, ser administrados e gerenciados por equipes integradas por servidores ou empregados públicos federais ocupantes de cargo efetivo ou militar de carreira, de órgão ou entidade da APF. Quando não for possível, a equipe pode ser mista, desde que sob a coordenação e responsabilidade de um servidor ou empregado público. (Ref.: 15/IN01/DSIC/GSIPR/2012)

7.13.4. Cabe ao CSIC estabelecer normas complementares para o Portal e contas de Redes Sociais Institucionais.

7.14. **Nuvem Computacional**

7.14.1. Nos termos da Norma Complementar nº 14/IN01/DSIC/GSIPR/2018, é possível a utilização e hospedagem de serviços e dados em Nuvem Computacional, desde que observadas as legislações vigentes.

7.14.2. A utilização de serviços em Nuvem é permitida apenas para atividades em consonância com os objetivos e metas do CEMADEN.

7.14.3. Cabe ao CSIC avaliar os riscos e deliberar sobre os projetos e soluções a serem implantadas em nuvem.

7.15. **Aplicativos Móveis**

7.15.1. É permitido ao CEMADEN desenvolver e disponibilizar aplicativos móveis, atendidas as determinações do Decreto nº 9.756, de 11 de abril de 2019.

7.15.2. Cabe ao CSIC estabelecer normas complementares para o desenvolvimento e disponibilização de Aplicativos Móveis.

8. PENALIDADES

8.1. O não cumprimento das determinações da POSIN sujeita o infrator às penalidades previstas na legislação e nos regulamentos internos do CEMADEN.

8.2. O usuário que fizer uso de forma indevida ou não autorizada dos recursos de tecnologia da informação e comunicações de dados, bem como agir em desacordo com os termos dessa política, fica sujeito à aplicação das penalidades previstas na Lei 8.112/90 e na legislação pertinente.

9. COMPETÊNCIAS E RESPONSABILIDADES

9.1. **Do Comitê de Segurança da Informação e Comunicações de Dados (CSIC)**

9.1.1. O CSIC será composto por um Gestor escolhido pela Direção e um membro representante de cada unidade constante no organograma da instituição, à ser indicado pelos respectivos Titulares das unidades e aprovados pela Direção.

9.1.2. O CSIC, de natureza consultiva, vinculado à Diretoria do CEMADEN, tem a finalidade de tratar sobre políticas, diretrizes, planejamento e demais ações relativas à Segurança da Informação e Comunicações de Dados (SIC) no âmbito das unidades constantes na estrutura organizacional do CEMADEN.

9.1.3. São competências do CSIC:

a) assessorar na implementação das ações de segurança da informação e comunicações de dados.

b) constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações de dados.

c) participar da elaboração da Política de Segurança da Informação e das Normas Internas de Segurança da Informação.

d) propor alterações na Política de Segurança da Informação do CEMADEN, em conformidade com as legislações existentes sobre o tema, bem como suas alterações, e submetê-la à Diretoria para aprovação.

e) propor normas relativas à segurança da informação e comunicações de dados.

f) deliberar sobre normas internas de segurança da informação.

g) exercer outros atos de assessoramento e de proposição afetos à matéria de segurança da informação e comunicações de dados.

9.2. **Do Gestor do Comitê de Segurança da Informação e Comunicações de Dados**

9.2.1. Compete ao Gestor do Comitê de Segurança da Informação e Comunicações de Dados do CEMADEN:

a) Coordenar o Comitê de Segurança da Informação e Comunicações de Dados (CSIC) e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR).

b) Coordenar a elaboração da Política de Segurança da Informação e das normas internas de segurança da informação do órgão, observadas as normas afins exaradas pelo Gabinete de Segurança Institucional da Presidência da República.

c) Assessorar a alta administração na implementação da Política de Segurança da Informação.

d) Estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação.

e) Promover a divulgação da política e das normas internas de segurança da informação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no órgão ou na entidade.

f) Incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação.

g) Propor recursos necessários às ações de segurança da informação.

h) Acompanhar os trabalhos da Equipe de Tratamento e Resposta a Incidentes Cibernéticos.

i) Verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação.

j) Acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação.

k) Manter contato direto com os órgãos pertinentes para obter auxílio sobre assuntos relativos à segurança da informação.

9.2.2. O Gestor do Comitê de Segurança da Informação e Comunicações de Dados e o seu substituto serão designados em portaria específica.

9.3. **Da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR)**

9.3.1. A ETIR tem a finalidade de facilitar, coordenar e executar as atividades de tratamento e resposta a incidentes em redes computacionais no ambiente do CEMADEN.

9.3.2. A ETIR do CEMADEN tem como objetivos básicos:

a) Monitorar as redes computacionais.

b) Detectar e analisar ataques e intrusões.

c) Tratar incidentes de segurança da informação.

d) Identificar vulnerabilidades e artefatos maliciosos.

e) Recuperar sistemas de informação.

f) Promover a cooperação com outras equipes, bem como participar de fóruns e redes nacionais e internacionais relativos à Segurança da Informação e Comunicações de Dados.

9.3.3. A ETIR será composta por servidores públicos, preferencialmente ocupantes de cargo efetivo, designados em portaria específica pelo Presidente do Comitê de Segurança da Informação e Comunicações de Dados do CEMADEN.

9.4. **Do Agente Responsável pela ETIR**

9.4.1. Compete ao Agente Responsável pela ETIR do CEMADEN:

a) Estabelecer os procedimentos operacionais, gerenciar as atividades e distribuir tarefas para a ETIR;

b) Assistir o CTIR GOV com informações necessárias à atualização e manutenção das bases de dados de incidentes do Governo Federal.

9.4.2. A equipe responsável pela área de Rede e Infraestrutura de Tecnologia da Informação e Comunicações de Dados do CEMADEN assumirá o papel de Agente Responsável pela ETIR.

9.5. **Dos Usuários e Colaboradores**

9.5.1. Compete aos usuários e colaboradores do CEMADEN:

a) Cumprir fielmente as políticas, as normas, os procedimentos e as orientações de segurança da informação e comunicações de dados do CEMADEN;

b) Buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à SIC;

c) Assinar Termo de Responsabilidade, formalizando a ciência e o aceite da POSIN do CEMADEN, bem como assumindo responsabilidade por seu cumprimento;

d) Proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados pelo CEMADEN;

e) Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pelo CEMADEN;

f) Comunicar imediatamente ao Comitê de Segurança da Informação e Comunicações de Dados (CSIC) qualquer descumprimento ou violação desta Política e/ou de seus documentos complementares.

10. ATUALIZAÇÃO

10.1. Esta Política bem como o conjunto de instrumentos normativos gerados a partir dela, será revisada de forma periódica ou sempre que se fizer necessário, não excedendo o período máximo de 03 (três) anos.

OSVALDO LUIZ LEAL DE MORAES
Diretor